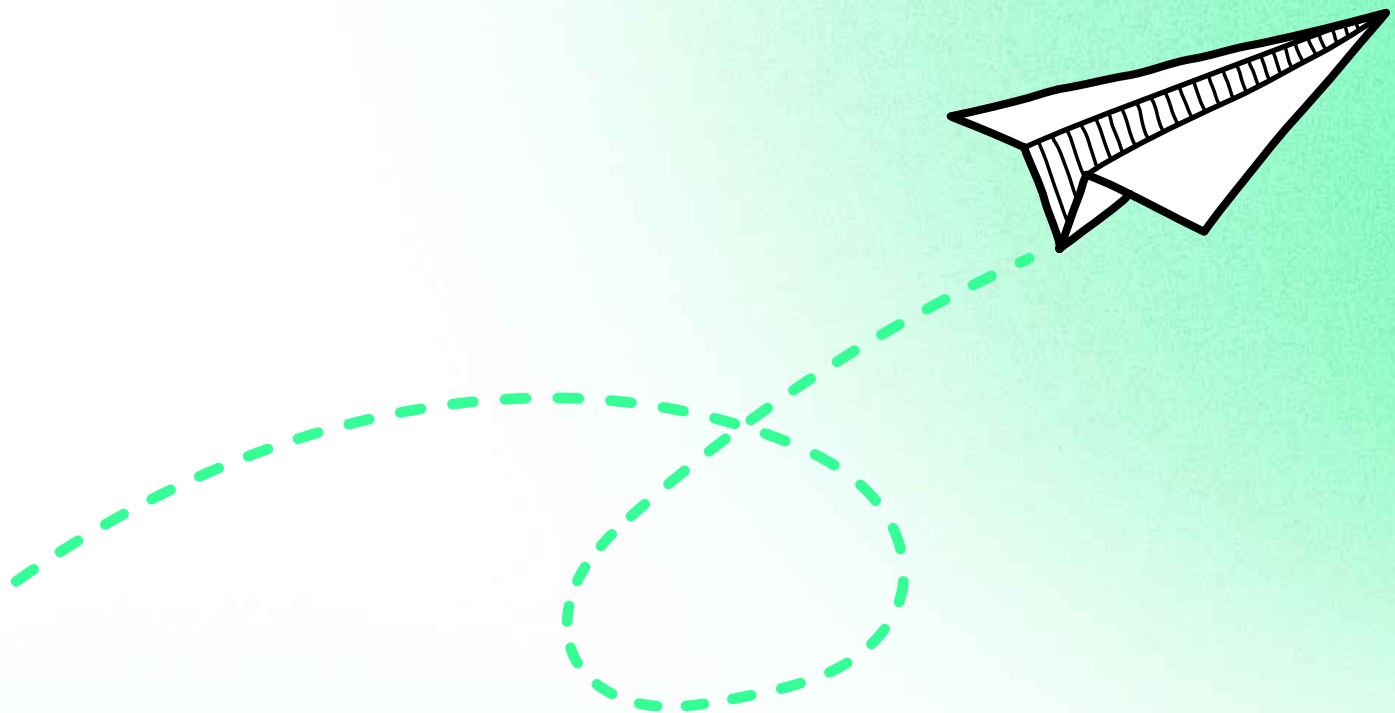# isms·online

The proven path to

ISO 27001

success

Quickly achieve and maintain ISO 27001 certification with features and tools designed to save you time, money and hassle.

ISO 27001

So, you need to get ISO 27001 certified.

If this is your first experience with the internationally recognised standard, you're probably wondering how to get started.

You may feel overwhelmed. That's understandable. It's a big standard with a lot of interconnected parts.

Don't worry. We help organisations worldwide with the most practical, affordable path to achieving and maintaining their ISO 27001 certifications every day. It's what gets us up in the morning!

In this guide, we'll help you understand:

- The basics of ISO 27001

- What a good Information Security Management System looks like

- How you can save time and budget by learning as you build

What is ISO 27001?

ISO 27001 is the only genuinely global information security management standard, so naturally, it's one of the most widely sought-after.

It applies to every industry and sets out how to design, build and implement an Information Security Management System (ISMS) that can be independently certified for assurance purposes.

As the world's best-known standard on information security management, ISO 27001 helps organisations secure their information assets – which is vital in today's increasingly digital world.

The standard is also regularly updated to ensure it meets the needs of the evolving information security threat landscape, with the most recent update taking place in 2022.
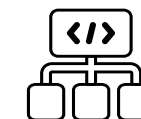
Benefits of ISO 27001

Internationally recognised

Internationally recognised best practice standard for information security management systems (ISMS)
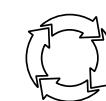
Risk-Based Approach

Provides a risk-based approach to information security management

Complete Framework

A framework to assist organisations in protecting the Confidentiality, Integrity and Availability of their most valuable assets

Continuous improvement process

A continuous improvement process (Plan/Do/Check/Act) to ensure your ISMS remains relevant

Influential customers and security-focused supply chains increasingly view ISO 27001 certification as a baseline requirement for doing business. It's no longer a 'nice to have; it's an expectation.

Why is ISO 27001 so important?

The importance of good information security practices in businesses cannot be overstated in today's digital world. ISO 27001 offers you the best possible protection for your information assets.

But it does so much more.

The IBM Data Breach Incident Report, in partnership with Ponemon, stated that the average global cost of a data breach reached USD $4.35 million in 2022, and 83% of organisations reported suffering more than one security breach in the last 12 months. With the increasing frequency and cost of cyber threats and data breaches, organisations must prioritise protecting their sensitive information. This is where the ISO 27001 framework can offer considerable benefits in the information security armoury.

ISO 27001 is an international standard for creating and maintaining an Information Security Management System (ISMS). The framework helps organisations evaluate their information security risks and implement mitigation controls. By using the ISO 27001 standard, organisations can improve their security posture, help enhance their brand reputation and improve customer trust creating a solid foundation for business growth.

Influential customers and security-focused supply chains increasingly view ISO 27001 certification as a baseline requirement for doing business. It's no longer a 'nice to have; it's an expectation.
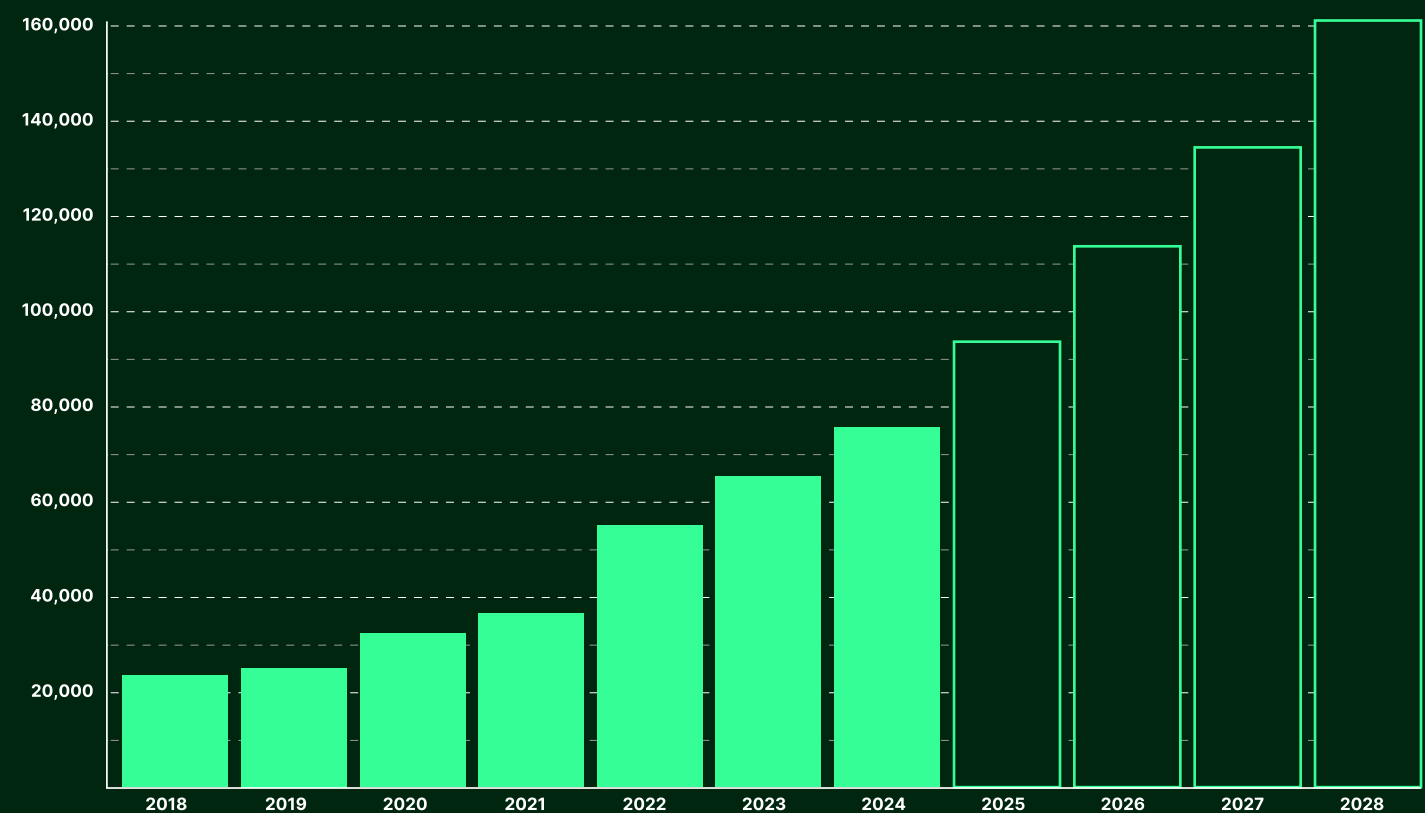
70%

of businesses have received fines for data breaches in excess of £100,000 in the last 12 months

ISMS.ONLINE STATE OF INFORMATION
SECURITY REPORT 2024

$4.8m

The global average cost of a data breach in 2024 — a 10% increase over last year and the highest total ever

IBM COST OF A DATA BREACH
REPORT 2024

Beyond trust

Today trust is no longer enough. You need certainty.

Trust is essential for any business. But in today's digital world, trust alone is not enough. Organisations need certainty in their information security practices. That's why more and more companies are choosing to get ISO 27001 certified, to demonstrate their ability to provide information security certainty to their customers and supply chains. In fact, certifications in ISO 27001 have risen by 450% over the last ten years.

As the only truly global information security standard, ISO 27001 is widely sought-after and applicable to all industries. It provides a framework for designing, building and implementing an Information Security Management System (ISMS) that can be independently certified for assurance purposes.

ISO 27001 certifications have risen by over 350% since 2018

That figure is projected to increase to over 700% by 2028

More than just cybersecurity

ISO 27001 empowers organisations to achieve a robust risk management posture that aligns with the digitisation of modern business practices and accompanying threats

ISO 27001 is more than just a security standard, it's a management standard that provides a framework for identifying and managing information security risks. It covers information security, physical security, cybersecurity, business improvement, business development, and data privacy.

The standard delivers a risk-based framework in two parts: **Clauses and Annex A controls**.

Clauses 4–10 detail the scope, definitions, and requirements for implementing and maintaining an ISMS.

Annex A provides 93 objectives and controls, divided into four categories: Organisational, People, Physical and Technological. **Each category has five attributes** aligned to with the common terminology used in information security.
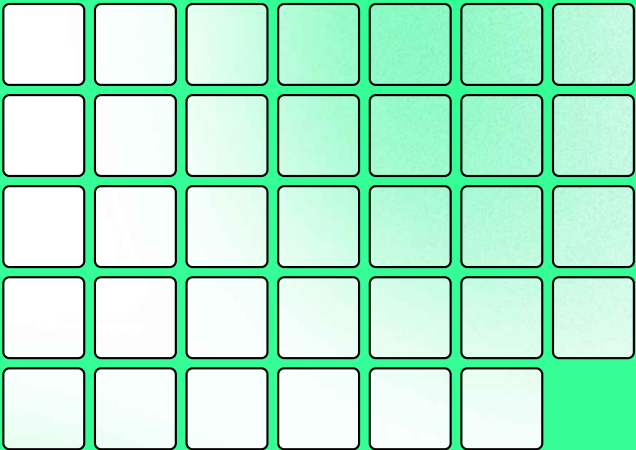
The five attributes are Control Types, Information Security Properties, Cybersecurity Properties, Operational Capabilities and Security Domains.

These attributes are used to manage and mitigate risks to the organisation and its supply chain.
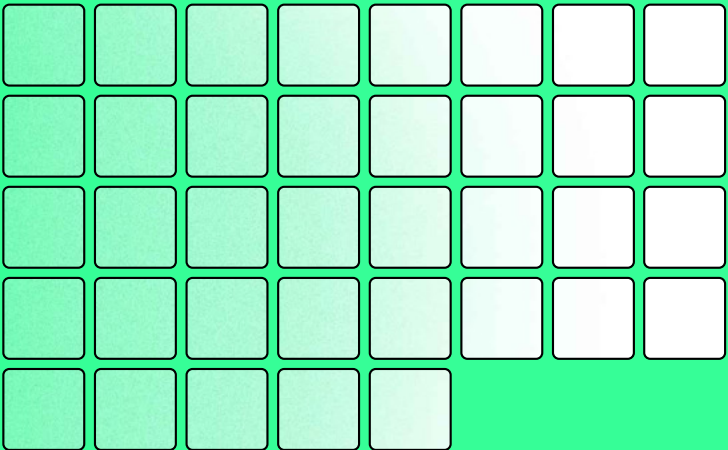
Physical Controls
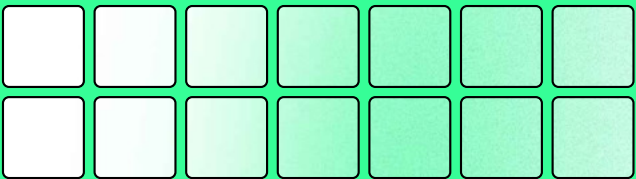
Technological Controls

People Controls

Organisational Controls

How do you reach certification?

Achieving ISO 27001 certification is the ultimate way to demonstrate your commitment to information security.

By creating an Information Security Management System (ISMS) that follows the ISO 27001 standard, you can be sure that your organisation is taking all necessary measures to protect sensitive information.

With our help, you'll pass through two rigorous external audits with ease, after which your auditor will recommend you for certification to the relevant accreditation body. Once certified, you'll enjoy the benefits of ISO 27001 for three years, with regular internal and external audits to ensure that you're always in compliance.

How long does it take?

We get asked this question a lot, and the truth is that it depends on two main factors – where you start and what approach you take.

In our recent State of Information Security Report, over 32% of organisations stated that it took them 1–5 years to achieve certification. Over 46%** of organisations use spreadsheets and toolkits to deliver the project.

In comparison, you can achieve success more quickly by using a pre-configured ISMS rather than by building your own, with the average time to complete sitting at less than six months (25%) and between 6-12 months (21%).*
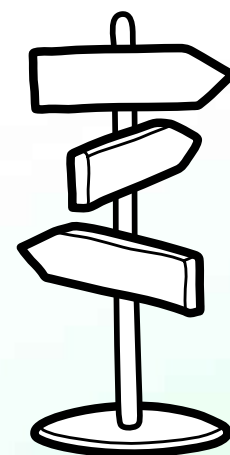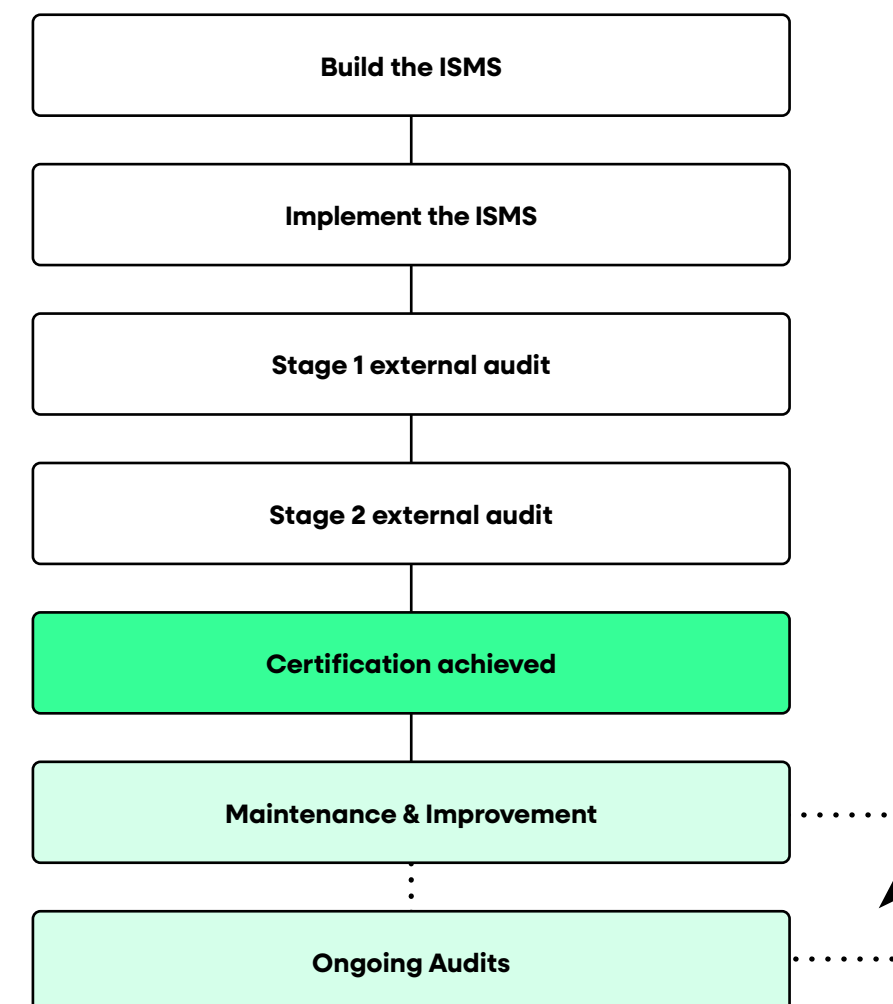
*Stats taken from the ISMS.online State of Information Security Report 2023 with a sample size of 500 professionals from senior-level information security positions

**Stats taken from a poll ran during our Simplifying Security Webinar, Nov 2022

ISO 27001 Certification Process

- Build the ISMS
- Implement the ISMS
- Stage 1 external audit
- Stage 2 external audit
- **Certification achieved**
- Maintenance & Improvement
- Ongoing Audits

Why do you need an ISMS?

An ISMS is an essential part of the compliance and certification process. It's difficult to achieve compliance or certification without one.

Implementing an ISMS is essential for any organisation as it showcases its commitment to information security. An ISMS outlines the procedures for identifying and addressing potential threats or opportunities related to the organisation's information and assets. Fundamentally, an ISMS is an essential element of a company's overall risk management strategy and helps to ensure the highest possible standards of information security, data confidentiality and company success.

In today's landscape, trust is everything. Implementing an Information Security Management System isn't just about compliance – it's about proving to customers and stakeholders that their data is handled with the highest level of integrity and care.

ISMS.online helps you align security with business goals while staying ahead of regulatory expectations.

Sam Peters
Chief Product Officer, ISMS.online

Avoid the big three mistakes

For organisations looking to achieve ISO 27001 quickly and realise the operational, financial and business benefits that certification delivers, avoiding common pitfalls is essential.
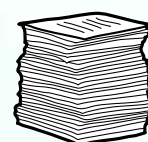
> **"**
>
> *ISMS.online has transformed the way we manage our ISO certifications. We've achieved a more efficient, centralised approach to managing compliance, allowing our team to focus on continuous improvement and proactive risk management, rather than administrative tasks.*
>
> **Charles M**
> Information Security Lead, Cinos
>
> **⟲ CINOS**

Don't rely on gap analysis

Instead of relying on a traditional gap analysis, consider using a pre-configured service that can immediately address common gaps. This will save valuable time and effort and provide an immediate return on investment.

Don't rely on a document toolkit

When managing your ISMS, avoid a basic toolkit approach. Instead, look for a solution that allows for easy creation, communication, control, and collaboration. This will ensure that you can approach ISO 27001 audits with confidence.

Don't start from scratch

Starting from scratch when building an ISMS is not the most efficient approach. It's similar to developing a bespoke sales or accounting system. Instead, look for existing off-the-shelf products that can save time, effort and budget.

The building blocks for an effective ISMS

If your ISMS doesn't have these characteristics as an absolute baseline, you'll end up with a less effective platform and working much harder than you need to.

A single source of truth

Make sure you choose a single software solution that's futureproofed for your ongoing compliance needs.

Works with your existing systems

Maximize efficiency by utilising integrations to streamline data collection and seamlessly connect with the software you already use daily.

Security confidence

You'll hold some very sensitive information in your ISMS so avoid software solutions with weak security.

Always accessible

Your ISMS should be available to authorised parties securely, when and where they want it, with backup and support as needed.

Easy to use

Keep it simple – complicated management systems are costly to use and encourage noncompliance.

Joined up

Choose a solution with easy navigation and clear linking to help stakeholders find their way.

Transparent

Impress your auditor with an ISMS that shows your working as it evolves, making it easy to record and track changes.

Collaborative

Go for built in collaboration tools to avoid duplication and help to demonstrate continual improvement.

Insightful and Actionable

An ISMS with pre-configured reporting and reminders will help you and your stakeholders make better decisions.

Affordable

Prove your return on investment with an ISMS that's cost effective to implement and operate.

Trusted worldwide

SIEMENS

BDO

Panasonic

moneycorp

Entain

FLIGHT CENTRE

NHS Professionals

TUI

pladis

rightmove

Coventry University

AtkinsRéalis

TRADE + INVESTMENT QUEENSLAND

RICOH imagine. change.

Winckworth Sherwood

ScottishPower

accountancy insurance

Orange Cyberdefense

"

ISMS.online is not only an expert in their field, but they are fast, efficient, and cost-effective. Their platform takes out a lot of the hard work and as they have a proven track record delivering this certification for many clients in the past, there are very few unknowns and surprises to deal with.

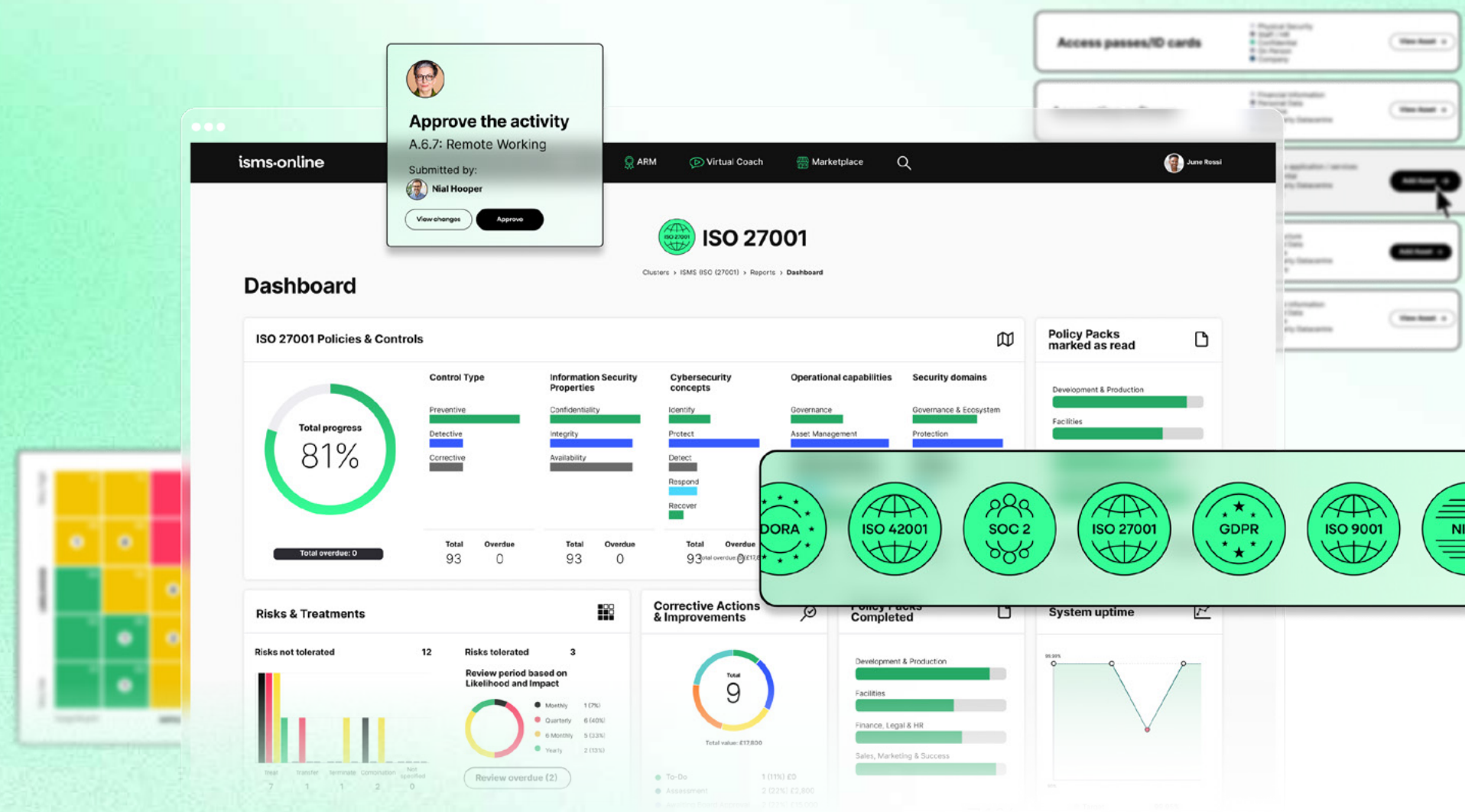**Andrew Conway** Chief Technology Officer, Xergy–Proteus

Book your platform demo today   Get started →

The ISMS.online solution

The fast lane to credible compliance

ISMS.online is packed full with all the tools, templates, and guidance you need to be compliant. And our expert support means help is always on hand when you need it.

Security, simplified.

Simplify your information security management with ISMS.online. Built with everything you need to succeed with ease, and ready to use straight out of the box – no training required!

The ISMS.online software platform has been expertly designed and has all the necessary tools and features to help you achieve and maintain ISO 27001 certification. With our comprehensive range of tools and content, we can assist in streamlining your ISO 27001 journey and help you attain success in a shorter timeframe.
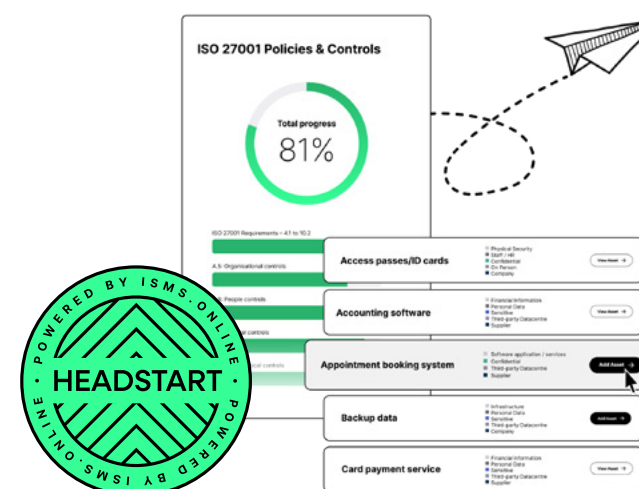
Start ahead, stay on top

With Headstart your journey to ISO 27001 is 81% complete from the moment you first log in. Simply adopt the preconfigured HeadStart content, adapt anything you need and then add in any specific policies and controls to fit your business.
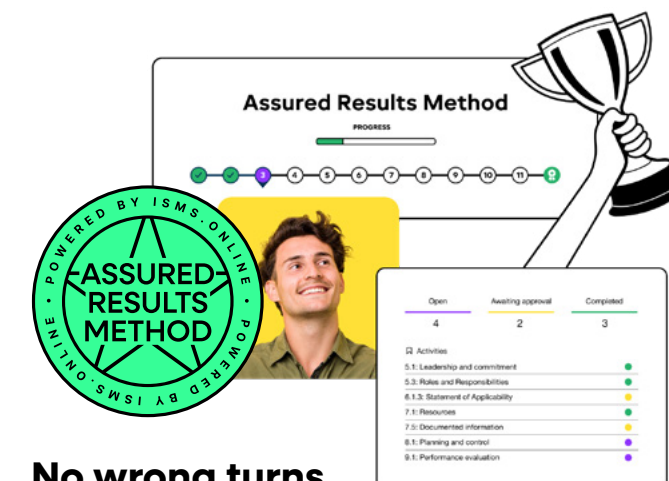
No wrong turns

Stay on track to certification with ARM, your Assured Results Method for ISO 27001 success. ARM takes all the ISO 27001 controls and breaks them down into 11 simple steps so you can achieve certification fast without any hassle or headaches.
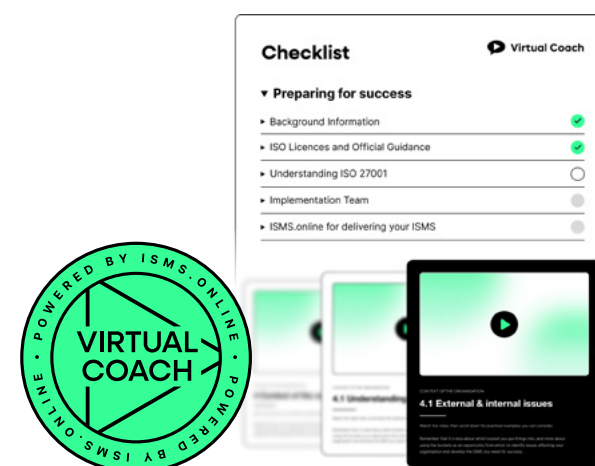
Your own ISO 27001 coach

Virtual Coach is there when you need any guidance on how to approach any aspect of ISO 27001. No need to wait for help, get your answers straight away with Virtual Coach – your always-on guide to ISO 27001 certification.

Works with your existing systems

No need to double your workload. Connect with over 5,000 apps and leverage the benefits of automating compliance by integrating ISMS.online with your existing tech stack. Integrate instantly, remove manual tasks, and let ISMS.online do the work for you.

Fast, seamless integrations

No need to double your workload. Integrate instantly with your existing setup, remove manual tasks, and let ISMS.online do the work for you.

Integrating compliance management tools into your business operations can streamline the compliance journey and achieve audit readiness.

With ISMS.online, businesses can go beyond simply outlining tasks and leverage the platform's automation capabilities to organise, remind, and capture corrective actions against each task continuously and in an audit friendly manner.

By leveraging our Zapier integrations, you can connect with over 5,000 other software platforms, enabling you to simplify the compliance journey from start to audit-ready and beyond. Moreover, ISMS.online is built and supported by security and compliance experts, assuring that the platform can handle compliance challenges effectively. By automating compliance management, businesses can simplify their security and compliance posture and confidently meet regulatory requirements.
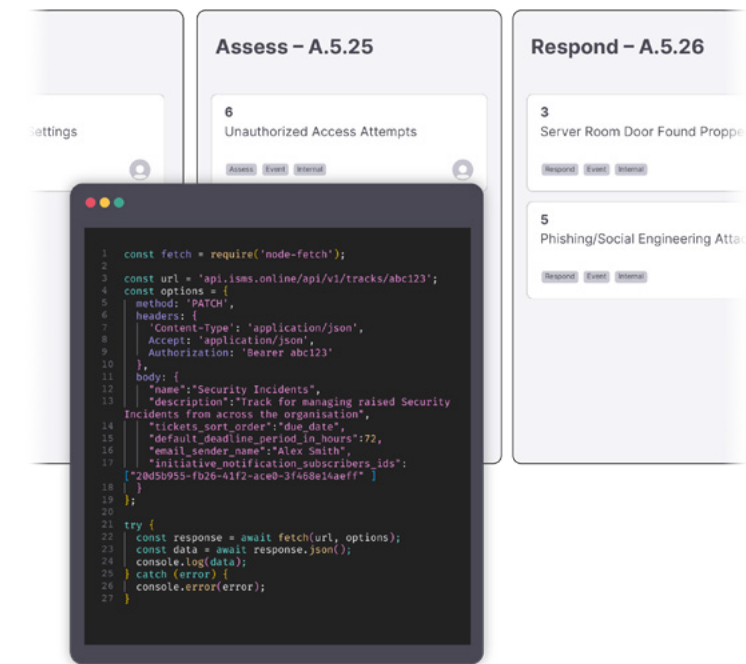
Take complete control with our Public API

With our Public API, you're in control, allowing you to integrate data from the platforms essential to your business operations and information security.

Looking to streamline your security incident management process by sending security incidents from Jira into ISMS.online? How about receiving a continuous feed of threats and vulnerabilities directly as track items? With the ISMS.online Public API, you can effortlessly connect these systems and many more while turning ISMS.online into your single point of truth for information security.

Our API is designed for simplicity, ensuring your development team can hit the ground running in minutes and enabling you to advance your information security initiatives with ease. Whether you prefer Python, JavaScript, Ruby, or other coding languages, we've got you covered. Our documentation has working code snippets in multiple languages, so you can play around and interact with the API easily.

Your complete compliance toolkit

ISMS.online features a dynamic and comprehensive toolset, built by experts to simplify every requirement of your ISMS build and maintenance.

If your ISMS is costing you time instead of saving it, it's time to move to ISMS. online. Every aspect of our simplified, secure, sustainable platform is designed to help you reclaim your time while giving you and your interested parties maximum assurance.

Easy Asset Management

Select assets from the Asset Bank and create your Asset Inventory with ease

Dynamic Risk Management

Effortlessly address threats & opportunities and dynamically report on performance

Perfect Policies & Controls

Easily collaborate, create and show you are on top of your documentation at all times

Mapping & Linking Work

Shine a light on critical relationships and elegantly link areas such as assets, risks, controls and suppliers

Fast, Seamless Integrations

Out of the box integrations with your other key business systems to simplify your compliance

Public API

Seamlessly integrate with key platforms to simplify your compliance by using ISMS.online's Public API

Staff Compliance Assurance

Engage staff, suppliers and others with dynamic end-to-end compliance at all times

Supply Chain Management

Manage due diligence, contracts, contacts and relationships over their lifecycle

Audits, Actions & Reviews

Reduce the effort and make light work of corrective actions, improvements, audits and management reviews

Interested Party Management

Visually map and manage interested parties to ensure their needs are clearly addressed

Clear Reporting

Make better decisions and show you are in control with dashboards, KPIs and related reporting

Localised for your needs

Need ISO 27001 policies and controls in French, German and Spanish? We've got you covered

Specialist support

As an ISMS.online customer you have access to a Live Support Team of platform experts and a Customer Success Manager who has a stake in your success.

You're busy and ISO 27001 is a big subject, so you may experience gaps in your capability, capacity or confidence. During your onboarding we help you identify what you currently have, what you may be missing and how quickly you're looking to achieve your goals. The outcome is a personalised roadmap that you can reference to ensure you're staying on track.

If at points you have trouble staying on target, our team of in-house specialists can step in to lighten the load.

"

The support team has been invaluable. They helped us migrate data, answered our everyday functionality questions, and their Information Security Experts were on hand to give us one-to-one support.

Dean Fields IT Director, NHS Professionals

"Our auditor loves it"

Ace your audits

Our platform ensures you can create, communicate, control and collaborate with ease – exactly the things your auditor will look for.

With your ISMS all-in-one-place and instantly accessible, you're perfectly placed to demonstrate the 'process of continual improvement' required by the foundational ISO 27001 standard.

With ISMS.online your compliance becomes 'business as usual' with all your activity creating clear audit trails. This means you'll approach every audit with confidence; knowing you've removed the risk of error while saving time and reducing cost.

★★★★★

"Our auditor LOVES it! Our initial certification audit was a breeze because ISMS.online made it easy to show her everything was in place."

Mark W.
Chief Technology Officer

★★★★★

"Turns the daunting task of ISMS compliance and certification into a surmountable one. I can't see how we would have achieved certification without it!"

L.K.
Project Manager

★★★★★

"ISMS.online is a game changer. Makes managing the system a breeze and helps with staying current and compliant."

Matthew F.
Director of Compliance

★★★★★

"ISMS.online has been vital to our success. The Assured Results Method is a neat and efficient system to keep track of our progress and has been instrumental to our success."

Vincent G.
Head of Compliance

Get started today

Book a demo →

A solution that grows with your business

With ISMS.online you can integrate any management systems that share common elements.

Easily compatible standards include ISO 27001, ISO 27701, ISO 9001, ISO 22301 and ISO 14001 and we can also help you bring together many other ISO and non-ISO standards into your system. In fact, we currently support over 100 standards, frameworks and regulations.
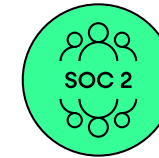
If we don't already cover what you're looking for, we can quickly and easily add them to our simple, secure and sustainable platform.

View all frameworks →

ISO 27001

The only truly global information security standard

Manage the security of consumer data by implementing an information security management system.
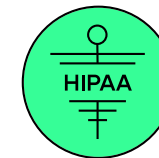
SOC 2

Protect and manage your customer data

SOC 2 outlines standards for the management of data with regards to: security, availability, processing integrity, confidentiality, and privacy.

ISO 27701

A framework to manage and protect personal data

ISO 27701 provides guidelines for the implementation of a privacy information management system.

HIPAA

Ensure the privacy of health records and personal information

HIPAA is a law that requires organisations managing protected health information to keep it secure and protected.

GDPR

Data protection and privacy in the EU and EEA

GDPR is an EU law establishing rules for the collection, use, and storage of personal data and individual rights related to their personal information.
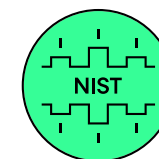
NIST

Reduce cybersecurity risk and protect networks and data

NIST is a US government standard that outlines the security requirements for protecting controlled unclassified information (CUI) in non-federal systems and organisations.

Feel compliance confident with

isms·online

Now that you understand the basics of ISO 27001 certification, book a chat with our product expert team to see how ISMS.online can help you grow your business.
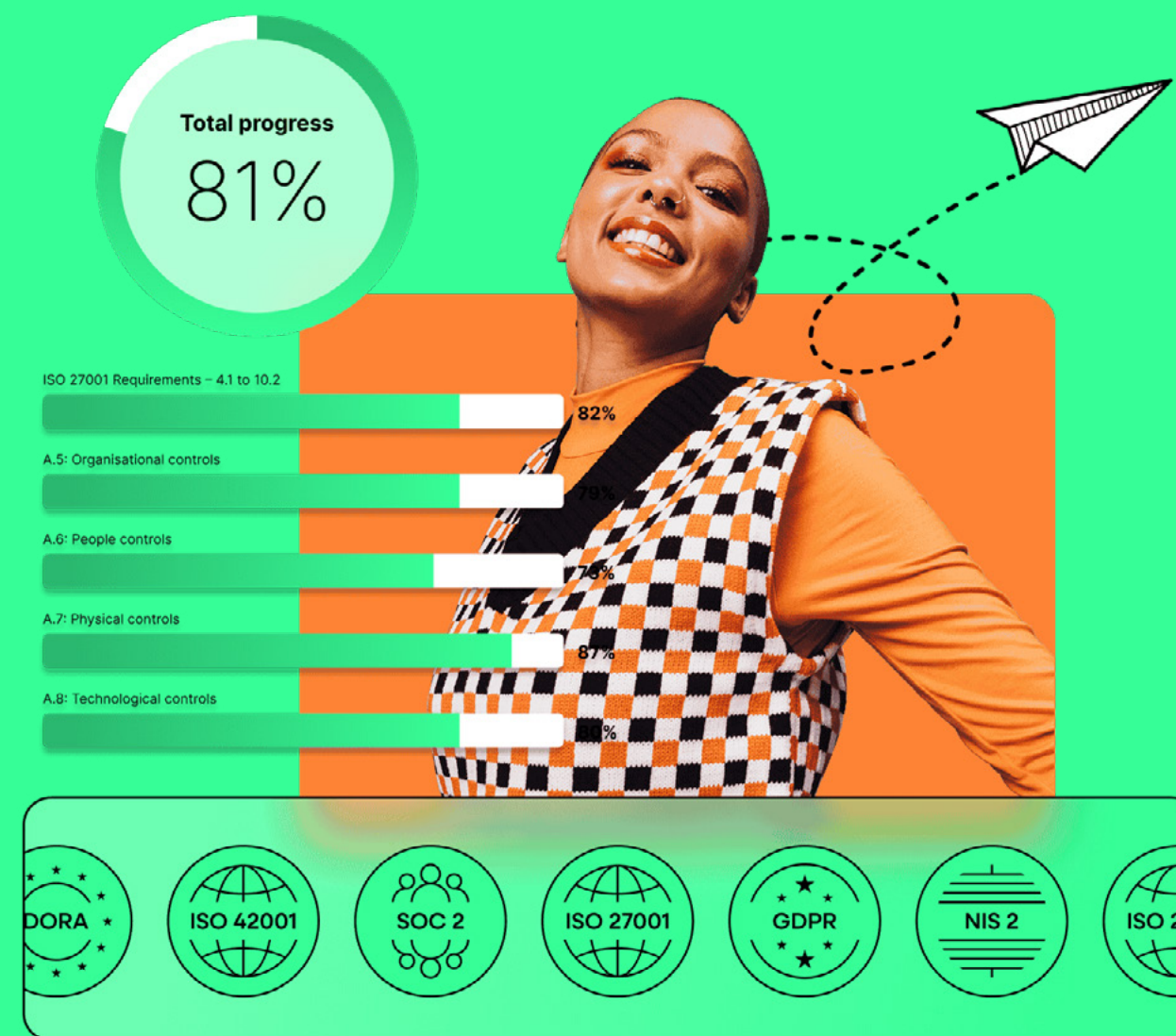
Start your compliance journey today — Get started →